REMARKS

Applicant appreciates the examination of the present application that is evidenced by the Official Action of June 23, 2004. Applicant also appreciates the indication Claims 6-10, 13, 19-20, 24, 29-31, 34-36, 43 and 48-49 recite allowable subject matter. In response to the Official Action, Applicant has addressed the rejections under 35 USC § 112 and has amended the specification. Many of the original claims have also been amended. In particular, original dependent Claims 6, 9, 13, 19, 24, 29, 34-35, 43 and 48 have been rewritten and amended as independent claims. In particular, Claims 6, 9, 13, 19, 24, 29, 34-35 and 43 have been amended to include recitations from respective independent claims and all intervening dependent claims. Claim 48 has also been amended to include recitations from independent Claim 44 (but not the intervening dependent Claims 45-47). Based on these amendments, Applicant respectfully submits that Claims 6-10, 13, 19-20, 24, 29-31, 34-36, 43 and 48-49 are in condition for allowance. Applicant will now address the outstanding rejections under 35 USC §§ 102, 103 and 112.

The recitation "first time interval" has been properly described in the specification

As described throughout the specification of the present application, the "first time interval" is identified as a time interval during which a plurality of data streams (e.g., encrypted data streams) are generated and an integrated circuit device (e.g., PLD) is operated. (See, e.g., p. 2, lines 24-29, p. 3, lines 1-6 and 11-13, p. 4, lines 14-19, p. 11, lines 5-10 and p. 12, lines 9-16 of the present application). For example, page 2 of the application provides the following description of how various data streams are generated while a PLD is simultaneously operated under control of program code during the first time interval:

> "According to a first preferred embodiment of the present invention, an integrated circuit system comprises an authorization device that generates an encrypted data stream and a

> programmable logic device (PLD) that also generates an encrypted data stream while simultaneously operating under at least partial control of program code during a first time interval." (Summary, p. 2, lines 24-29).

At page 3 of the application, the authorization detection circuitry is described as comparing "the encrypted data streams at least periodically during the first time interval." This comparing operation occurs while the encrypted data streams are being generated: "the second stream encryptor 100 within the authorization device 56 may use conventional permuting operations to sequentially determine a plurality of permuted bits as {H1, H2, H3, ..., Hn} during a first time interval." (See, e.g., page 11, lines 5-7). Finally, at page 12, lines 9-16 of the present application, the following passage is provided, which highlights how multiple data streams are generated and compared while a PLD is running proprietary software:

> "The second and third encrypted data streams R and R' are evaluated at least periodically during the first time interval to determine whether a "match" is present between the authorization device 56 and the proprietary "software" loaded into the PLD 54. This evaluation is preferably performed by the authorization detection circuitry ADC 84 within the PLD 54. Thus, a direct ongoing comparison can be made between the encrypted data streams to determine whether there is a sufficiently close identity therebetween, while the PLD 54 is running the proprietary software." (Description, p. 12, lines 9-16, underline added).

Based on this discussion, Applicant respectfully requests that the rejections of Claims 1, 16-17, 20-22, 26-27, 32 and 37 based on 35 USC § 112, first paragraph, be withdrawn.

The recitation "weakly random sequence of bits" has been properly described

The present application provides ample description of how to generate a "weakly random sequence of bits" and a degree of "randomness" to be associated with such a sequence, which is frequently also referred to as a "pseudo-random" sequence to those skilled in the art. Obviously, in most commercially viable circuits and systems, it is not practical to generate a perfectly random sequence of bits because this level of randomness requires highly complex and computationally expensive algorithms. Nonetheless, the weak random data generator 70 at page FIG. 4A of the present application, which mixes a "periodic" clock signal (CLK) with a "random" noise signal (NOISE) to thereby generate a "weakly" random output, uses a computationally inexpensive algorithm and is even described as possibly being of conventional design. (See, e.g., p. 7, lines 26-30 and p. 10, lines 13-20). Thus, based on this description, one of ordinary skill in the art would be well aware of techniques to generate "weakly" random data streams and would well understand the degree of randomness associated with such data streams. At page 10 of the present application, the term "weak" is used to describe an imperfect level of randomness (i.e., pseudo-randomness):

> "... As described above with respect to the weak random data generator 70 in FIG. 4A, a first data stream P may be generated by mixing noise and clock signals. This mixing operation may be performed using conventional techniques using an "unpredictable" circuit that sequentially generates a weak pseudo-random stream of bit data as {P1, P2, P3, ..., Pn), where "n" is an integer." (Description, p. 10, lines 15-20).

Accordingly, the application clearly describes a weakly random sequence of bits as a pseudo-random sequence having a degree of randomness that is comparable to that which can be obtained using computationally inexpensive algorithms, such as by mixing a plurality of signals (e.g., clock and noise signals).

Based on this discussion, Applicant respectfully requests that the rejections of Claims 14-15, 17, 19-20, 22, 24-25, 29-31, 45-47 and 50 based on 35 USC § 112, first paragraph, be withdrawn.

The Specification has been amended to recite "dead man switch"

As requested by the Examiner, the detailed description of the application has been amended to accord with the language of original Claims 19, 24 and 43. In particular, page 7 of the application has been amended to recite "dead man switch." Accordingly, Applicant respectfully requests withdrawal of the rejections of Claims 19, 24 and 43 under 35 USC § 112.

The Specification clearly describes "points in the first time interval"

The application describes the sequential generation of data bits (e.g., permuted bits: H1, H2, ..., Hn) during a first time interval. Based on this description, each data bit must be generated at a respective time "point" in the time interval. Nonetheless, in response to the Examiner's request, page 11 of the specification has been amended with the Examiner's proposed language: "a respective point in the first time interval."

Claim 38 has been amended to recite "a group consisting of ...."

Claim 38 has been amended to correctly recite a Markush group. Thus, instead of reciting "the group consisting of ....", Claim 38 now recites "a group consisting of ..."

Claims 1-5, 11-12, 14-18, 21-23, 25-28, 32-33, 37-42, 44-47 and 50 are patentable over the cited references

Applicant admits some confusion over the citation of U.S. Patent No. 5,652,793 to Priem et al. as a primary reference to reject the above-identified claims. As described throughout the present application, Applicant's embodiments of the invention provide a form of continuous and ongoing authorization of the operation of an integrated circuit device. This continuous and

ongoing authorization provides a much higher degree of security against unlawful software copying because it requires the continuous monitoring by an authorization device during any operation of an integrated circuit device containing proprietary software. (See, e.g., device 56 and 56a in FIGS. 3A-3C). Thus, for each copy of software purchased by a user, an accompanying "authorization" device must also be purchased to provide continuous authorization.

In stark contrast, Priem et al. provides an authorization operation that occurs only prior to running a software program and not continuously while the software program is operating. Once the software program in Priem et al. has been authorized and commences operation, there is nothing that precludes reverse engineering (e.g., theft) of the plaintext value and key stored in EEPROMs 22 and 24 or the password stored in the password storage unit (coupled to the compare circuit 30) or the encoding circuit 26 so that additional unlawful software copies can also be authorized. Priem et al. provides absolutely no disclosure of how to prevent improper authorization of multiple identical copies of proprietary software once a secret key and password have been reverse engineered.

All of these limitations of Priem et al. are addressed by the embodiments of the present invention and the above-identified claims clearly recite patentable distinctions vis-a-vis Priem et al. For example, Claim 1 recites that a first data stream and a second encrypted data stream are both time-varying during at least a first time interval. These data streams are evaluated at least periodically at multiple points during the first time interval to assess whether concurrent operation of a programmable logic device is authorized during this same time interval. Priem et al. provides absolutely no disclosure or suggestion of this type of ongoing authorization using data streams that are time-varying during the period when the logic device is operating and undergoing authorization.

Finally, Applicant objects to the Examiner's assertion at page 4 of the Official Action that "during a first time interval" corresponds to the "beginning of the running of a program." In Priem et al., the single event authorization is performed

only once prior to commencement of any authorized running of a program and not continuously thereafter using time-varying data streams. However, in the claims, the recited time interval corresponds to the operation of the device as well as the ongoing authorization operations, which are performed concurrently with the operation of the device.

In addition to Claim 1, all of the other rejected independent Claims 16, 21, 26, 32, 37 and 44 have been amended to clarify the timing overlap between the time-varying data streams, which Priem et al. does not describe, the authorization operations and the operation of an integrated circuit device (e.g., PLD, ASIC). Applicant also submits that the Examiner's citation of multiple secondary references to reject dependent claims is improper because none of these references reasonably disclose or suggest proper combination with Priem et al. in a software authorization environment. Thus, these dependent claims are independently patentable.

CONCLUSION

Applicant has shown that the continuous authorization techniques provided by embodiments of the present invention are materially different from the disclosure of Priem et al., which merely shows a single comparison operation using static data (i.e., password, plaintext value, etc.) that may be readily reverse engineered and copied so that additional unlawful copies of a software program may be operated. Applicant has also amended the specification as requested by the Examiner. Accordingly, Applicant submits that the present application is in condition for allowance, which is respectfully requested. The Examiner is strongly encouraged to contact the undersigned in the event any issues remain which may prevent issuance of the present application.

Respectfully submitted,

Grant J. Scott
Registration No. 36,925